UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

UNITED STATES OF AMERICA	:	
	:	
vs.	:	INDICTMENT NO.
	:	
TREMAINE GRANT,	:	4:23CR-096-001
	:	
Defendant.	:	

MOTION TO SUPPRESS WIRETAP EVIDENCE

COMES NOW, Tremaine Grant, by and through counsel, and pursuant to Federal Rule of Criminal Procedure 12(b)(3)(C), respectfully moves this Court for an evidentiary hearing and an order suppressing the wiretap evidence and any evidence derived from the wiretaps in the case. Mr. Grant moves to suppress evidence from both his telephone communications, as well as evidence that is derived from said communications which were obtained in violation of his First, Fourth, Fifth, Sixth or Fourteenth Amendment rights, 18 USC § 2234, 18 USC § 2510 *et seq.*, or Fed.R.Crim.P. 41. In support of this Motion, Mr. Grant relies upon all matters that are properly before the Court when this Motion is considered, and further shows the following:

I. FACTUAL BACKGROUND

On March 10, 2023, the government made application for and was granted an order authorizing the interception of wire and electronic communications and geolocation data for cellular telephone number 912-658-8086, which was referred to as "Target Telephone 1" or "TT1", and cellular telephone 912-438-1273, which was referred to as "Target Telephone 2" or "TT2." Said numbers are alleged to be used by Laron Thompson and Donald Davis, respectfully. Subsequently, on April 7, 2023, the government made

application for and was granted an extension order for Target Telephone 2.

Furthermore, in the same April 7, 2023 Application and Order, the government was granted an order authorizing the interception of wire communications and geolocation data for cellular telephone number 912-358-9223, which was referred to as "Target Telephone 3" or "TT3", cellular telephone number 912-401-5809, which was referred to as "Target Telephone 4" or "TT4", and cellular telephone number 470-910-8624, which was referred to as "Target Telephone 5" or "TT5." Target Telephone 3 and Target Telephone 4 are alleged to be used by Tremaine Grant.

II. CITATION TO AUTHORITY

A. Standing

Pursuant to 18 U.S.C. § 2510(11) an "aggrieved person" is a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.

Pursuant to 18 U.S.C. § 2518(10), any "aggrieved person" may move to suppress the contents of any wire or oral communication intercepted on the grounds that (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

The Supreme Court has interpreted these provisions as limiting standing to challenge wiretaps to persons whose Fourth Amendment rights were violated by the interception. *Alderman v. United States*, 394 U.S. 165, 175-76, n.9 (1969).

B. Statutory Requirements

The federal procedure for the interception of wire, oral or electronic communications is listed in 18 U.S.C. § 2518. This statute requires an application for an order authorizing the interception of electronic communications be submitted. Each application requires a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, and (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted, 18 U.S.C. § 2518(1)(b).

The application further requires a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; and a statement of the period of time for which the interception is required to be maintained.

If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving

any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results. 18 U.S.C. § 2518(1)(c), (d), (e) and (f).

A court, if presented with an appropriate application, may only issue an order for interception of private communications if (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this Title III; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and (d) there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. *See* 18 U.S.C. § 2518(3).

Should all of these requirements be met, a court may issue an order pursuant to 18 U.S.C. § 2518(4) specifying (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and (e) the period of

time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

Every order and extension thereof shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *See* 18 U.S.C. § 2518(5). Additionally there is a post-authorization duty of timely sealing or recordings. *See* 18 U.S.C. § 2518(8).

C. Case Law Requirements

1. Probable Cause

To support an order for electronic surveillance, an affidavit must establish among other things, probable cause to believe that an individual is committing, has committed, or is about to commit certain offenses enumerated in 18 U.S.C. § 2516, and probable cause to believe that communications concerning that offense will be obtained through electronic surveillance. 18 U.S.C. § 2518(3)(a). The probable cause necessary to support a wiretap authorization is the same probable cause necessary for a search warrant. *United States v. Nixon*, 918 F.2d 895, 900 (11th Cir. 1990). Thus, probable cause only exists if after a review of the totality of the circumstances, the court determines there is a fair probability that the evidence sought will be obtained. *Illinois v. Gates*, 462 U.S. 213, 239 (1983). An application for an order of electronic surveillance must establish probable cause for *each* telephone. *United States v. Carneiro*, 861 F.2d 1171, 1176-77 (9th Cir. 1988) (emphasis added).

2. Necessity Requirement

A separate and distinct prerequisite to the issuance of an order authorizing the interception of electronic communications has been termed the "necessity requirement". Separate from a probable cause requirement, the "necessity requirement" must be satisfied before a wiretap order may be lawfully issued. *See* 18 U.S.C. §§ 2518(1)(c) and (3)(c). Wiretap surveillance is *not* intended to be "routinely employed as the initial step in a criminal investigation, [r]ather, the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *United States v. Giordano*, 416 U.S. 505, 515 (1974). The purpose of the necessity requirement is to ensure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime. *United States v. Kahn*, 415 U.S. 143, 153 n. 12 (1974). The statute does not "foreclose electronic surveillance until every other imaginable method of investigation has been unsuccessfully attempted," *United States v. Alonso*, 740 F.2d 862, 868 (11th Cir. 1984); however, it does require the Government to show why alternative measures are inadequate for "this particular investigation." *United States v. Carrazana*, 921 F.2d 1557, 1565 (11th Cir.1991). *See, e.g., United States v. Perez*, 661 F.3d 568, 581 (11th Cir. 2011).

Mere conclusions by the affiant are insufficient to justify the necessity requirement for issuance of a wiretap order. *Cf., Aguilar v. Texas*, 378 U.S. 108 (1964) (reviewing search warrant affidavits). Further "generalities, or statements in the conclusory language of the statute, are insufficient to support a wiretap application". *United States v. Castillo-Garcia*, 117 F.3d 1179, 1188 (10th Cir. 1997). Similarly,

"boilerplate conclusions that merely describe inherent limitations of normal investigative procedures," (*United States v. Blackmon*, 273 F.3d 1204, 1210 (9th Cir. 2001)) or that are based solely upon an agent's knowledge and experience rather than the facts of a specific case are insufficient to establish necessity. *United States v. Spagnuolo*, 549 F.2d 705, 710 (9th Cir. 1977). Instead, "the statements must be factual in nature and they must specifically relate to the individuals targeted by the wiretap," *Blackmon* at 1210. *See* also *United States v. Perez*, 661 F.3d 568 (11th Cir. 2011); *United State v. Carrazana*, 921 F.2d 1557 (11th Cir. 1991); *United States v. Ippolito*, 774 F.2d 1482 (9th Cir. 1985); *United States v. Robinson*, 698 F.2d 448 (D.C. Cir. 1983); *United States v. Kalustain*, 529 F.2d 585 (9th Cir. 1976).

Finally, each wiretap application or extension, standing alone, must satisfy the necessity requirement. *United States v. Carneiro*, 861 F.2d 1171, 1176 (9th Cir. 1988).

3. Minimization Requirement

18 U.S.C. § 2518(5) instructs that surveillance be conducted in such a manner as to minimize the interception of non-relevant conversations, with this requirement being applicable to each initial and extension order. Compliance with the minimization requirement requires review of each case based on its individual facts and circumstances. *Scott v. United States*, 436 U.S. 128.

To assess the Government's compliance with the minimization requirement a hearing is necessary where the Government must bear the burden of proof regarding proper minimization (*see United States v. Rizzo*, 491 F.2d 215, 217, n.7 (2nd Cir. 1974), including (1) the number and identification of intercepted conversations; (2) whether intercepted conversations were "coded"; (3) if "coded", the efforts and techniques

utilized in "decoding" such conversations; (4) whether "decoding" occurred at the time of the conversation or after; (5) whether the "two-minute" rule was utilized by the Government in minimization; (6) how soon after the termination of a conversation minimization occurred; (7) who accomplished minimization; and (8) whether and when there was judicial review of the progress related to minimization.

4. Sealing Requirement

18 U.S.C. § 2518 (8)(a) requires that "immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions…" In the absence of immediate sealing, the recordings must be suppressed absent a satisfactory explanation from the Government stating why the delay occurred and why it is excusable. Simply providing proof of nontampering is not a substitute for strict adherence to the sealing provision. *United States v. Ojedo Rios*, 495 U.S. 257, 254-65 (1990).

"Immediate" has not been defined as a certain number of days, but the law tends to endorse sealing within one or two days of the expiration of the order. *See United States v. Matthews*, 431 F.3d 1296 (11th Cir. 2005).

III. ARGUMENT

A. Standing

Mr. Grant is an aggrieved person as defined by to 18 U.S.C. § 2510(11) in that he was a person who was a party to an interception and subsequently a person against whom an interception was directed. Specifically, the initial order for interceptions was granted regarding telephone number 912-438-1273 ("TT2") allegedly belonging to Donald Davis. Calls were intercepted pursuant to this original order to which Mr. Clark was a party.

Subsequently, the original order regarding telephone number 912-438-1273 ("TT2") was extended.

Additionally, the Government made application for and was granted an order authorizing the interception of wire communications regarding 912-358-9223 ("TT3"), and cellular telephone number 912-401-5809 ("TT4"), belonging to Mr. Grant and communications were intercepted.

As an aggrieved person, Mr. Grant may move to suppress the contents of any wire or oral communications. As such, pursuant to Fed.R.Crim.P. 12(b)(3), 18 U.S.C. §§ 2515 and 2518, and the Fourth Amendment to the Constitution of the United States, Mr. Grant moves to suppress the contents of any wire or oral communicated intercepted pursuant to a court order, as well as any evidence derived therefrom on the grounds that:

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; and

(iii) the interception was not made in conformity with the order of authorization or approval.

B. The Applications and Orders for Wiretap Fail to Comply with the Requirements of 18 U.S.C. § 2518(1)(b) and (4).

18 U.S.C. § 2518(1)(b) provides in relevant part that each application shall include a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (ii)…a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted.

In turn, 18 U.S.C. § 2518(4)(b) requires that each order authorizing and approving the interception of any wire, electronic, or oral communication shall specify the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted.

The initial application fails to provide a *particular* description of the nature and location of either the facilities from which or the place where the communication is to be intercepted. In fact, page six (6) of the Application related to Target Telephone 1 and Target Telephone 2 simply lists "**[service provider(s)]**" in the paragraph requesting information pursuant to U.S.C. § 2518(4).

C. The Applications and Orders for Wiretap Orders were not supported by probable cause.

The Application for Interception of Wire and Electronic Communications and the Application for Order Extending the Period of Authorized Interception of Wire and Electronic Communications were not supported by probable cause and did not meet the other requirements of Title III.

First of all, in Paragraph "19" of the Affidavit of Bradley Fisk in support of the Government's Application for Interception of Target Telephone 1 and Target Telephone 2, he specifically notes that a "Basis of Information" is the telephone toll records, pen register and trap and trace information, and telephone subscriber information. However, the various Applications for Orders Authorizing the Installation and Use of Pen Register and Trap and Trace Devices fail to outline the cell phone number in question. Although the Applications reference someone's name (Malik McKenzie, Laron Thompson, Donald Davis, Tremaine Grant, etc.), they fail to include Attachment A which is referenced in the

Applications; and consequently, they lack a phone number to which the Application makes a request.

Moreover, an entire section of the Affidavit is labelled "Analysis of Telephone Records for Target Telephone 1 and Target Telephone 2". As noted above, the evidence obtained via pen register and trap and trace devices should be excluded as the Applications for such information fail to identify any particular phones and solely refer to Attachment A, which does not exist in the filed Applications.

Furthermore, the initial application and order for wiretap issued in this investigation were based on information provided by two confidential human sources. The affidavit on which this application was based failed to outline sufficient evidence proving that these two confidential human sources and their proffered evidence was reliable. Furthermore, the information provided by these sources was largely uncorroborated. A search warrant based upon information obtained through confidential informants can only be issued upon a probable cause showing that the informant and his or her information are reliable. As the probable cause necessary to support a wiretap authorization is the same as that necessary for a search warrant, the initial order in this case should fail because the court could not determine that the information provided by the confidential human sources was reliable.

To highlight this fact, it is specifically learned that one of the confidential human sources on which the initial application was based is *not* reliable because the source is not credible. Specifically, the source fabricated a threat for his own gain, and when this fabrication was ultimately discovered by law enforcement, the use of the source was necessarily ceased and an investigation and recommendation for prosecution was

initiated. Since all subsequent applications are based upon the information obtained as a result of the initial wiretap order, it follows that all subsequent orders should fail.

Furthermore, the affidavits that were submitted with the aforementioned applications were supported by stale information with some information relating back in time in excess of five (5) months. Because the wiretap orders were not supported by probable cause, but rather stale, unreliable and uncorroborated information, all evidence obtained as a result of the wiretaps in this case should be suppressed.

D. The Necessity Requirement has not been met.

A separate and distinct prerequisite to the issuance of an order authorizing the interception of electronic communications has been termed the "necessity requirement". Separate from a probable cause requirement, the "necessity requirement" must be satisfied before a wiretap order may be lawfully issued. *See* 18 U.S.C. §§ 2518(1)(c) and (3)(c).

The applications and orders in the instant case are insufficient on their faces, as they fail to show that other investigative techniques have failed or why they reasonably appear to be unlikely to succeed if tried. In fact, the initial application in the investigation referencing Target Telephone 2 shows that substantial inroads were being made into the investigation through normal investigative techniques and procedures. Investigators were successfully employing the use of confidential sources, successfully conducting controlled buys and successfully consensually recording telephone conversations. Additionally, Investigators were successful in conducting physical surveillance through the use of pole cameras and in-person surveillance. Investigators did not however attempt further methods of physical surveillance, did not utilize

undercover agents, they did not conduct a grand jury investigation despite having at least two potential witnesses available (persons used as confidential human sources), they did not conduct any trash pulls, and they did not do any mail covers. Financial investigations were begun, but such investigations were not given sufficient time to produce fruitful information. The abandonment of financial investigations seems questionable, especially when the initial target offenses included allegations of money laundering.

Furthermore, the search warrants that were used specifically for cell phones did result in information related to marijuana distribution from Los Angeles to Savannah. Additionally, the Affidavit concedes that interviews have been effective in gathering information on the membership and operation of the DTO, and in fact led to the recruitment of a confidential source. Investigators argue that offering immunity to some witnesses would result in some of the most culpable people not being prosecuted, but this argument falls flat when the central argument supporting the wiretap investigation is to discover the more culpable people in the DTO. The justification included in the applications for moving from traditional investigative techniques to the utilization of wiretaps are, at best, mere conclusions, generalities and boilerplate that do not specify why wiretaps are necessary in this particular investigation and related to this Defendant.

This scenario is a situation in which a traditional investigation was successful and would have sufficed to expose the crime. However, investigators chose to almost completely desert normal investigative techniques in favor of wiretaps. Furthermore, subsequent wiretap applications submitted in this investigation rely almost exclusively on the information obtained as a result of preceding wiretap orders with very little

independent investigation through traditional investigative practices, to the point that there is almost no normal investigation once the electronic surveillance commences. As such, the initial order as to Target Telephone 1 and Target Telephone 2 should fail, as well as the extension of Target Telephone 2 and the initial order for Target Telephone 3, Target Telephone 4, and Target Telephone 5.

E. The Minimization Requirement has not been met.

Upon information and belief, law enforcement agents failed to comply with the minimization requirement of 18 U.S.C. § 2518(5). The burden is on the government to show proper minimization in this case.

Upon information and belief, the government substantially failed to minimize non-pertinent calls as a whole in this case, which allows an inference that the government engaged in an essentially warrantless, general search, warranting the suppression of all intercepted calls. Of note is the lack of minimization on March 14, 2023, for a period in excess of six (6) hours on Target Telephone 2, as well as the presence (albeit brief) of an unminimized TFO being present in the wire room during the extension of Target Telephone 2 and the initial interception of Target Telephone 3, Target Telephone 4, and Target Telephone 5.

F. The Sealing Requirement has not been met.

Upon information and belief, the recordings made as a result of these wiretaps were not sealed in accordance with 18 U.S.C. § 2518 (8)(a). The immediate sealing and storage of recordings of intercepted conversations under the supervision of a judge, is an integral part of the statutory scheme. In the absence of immediate sealing, the recordings must be suppressed absent a satisfactory explanation from the government stating why

the delay occurred and why it is excusable. Simply providing proof of nontampering is not a substitute for strict adherence to the sealing provision. *United States v. Ojedo Rios*, 495 U.S. 257, 254-65 (1990). In this case, the government came into possession of Target Telephone 3 and Target Telephone 4 on April 21, 2023. At that point, there was not any additional information to be obtained from monitoring; however, surveillance was conducted through April 24, 2023, and the records were not submitted for sealing until April 26, 2024.

IV. CONCLUSION

WHEREFORE, Mr. Grant respectfully requests this Court to grant an evidentiary hearing and suppress any and all evidence improperly obtained as a result of the wiretap orders and the extensions thereof.

Respectfully submitted, this 7th day of April, 2024.

/s/ M. P. Hicks, III
M. P. "Trey" Hicks, III
Attorney for Mr. Grant
Georgia State Bar Number: 351337

M. P. Hicks, III P.C.
P. O. Box 31348
Sea Island, GA 31561
770.490.2049
770.884.8131 - fax
thehickslawfirm.trey@gmail.com

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

UNITED STATES OF AMERICA	:	
	:	
vs.	:	INDICTMENT NO.
	:	
TREMAINE GRANT,	:	4:23CR-096-001
	:	
Defendant.	:	

CERTIFICATE OF SERVICE

The undersigned certifies that I have on this day served all the parties in this case with the foregoing MOTION TO SUPPRESS WIRETAP EVIDENCE in accordance with the notice of electronic filing ("NEF") which was generated as a result of electronic filing in this court.

This 7th day of April, 2024.

/s/ M. P. Hicks, III
M. P. "Trey" Hicks, III
Attorney for Mr. Grant
Georgia State Bar Number: 351337

M. P. Hicks, III P.C.
P. O. Box 31348
Sea Island, GA 31561
770.490.2049
770.884.8131 - fax
thehickslawfirm.trey@gmail.com